arXiv:0807.2234v2 [quant-ph] 19 Nov 2009

Quantum cryptography using partially entangled states

Goren Gordon[a] and Gustavo Rigolin[b,1]

[a] Department of Chemical Physics, Weizmann Institute of Science, Rehovot 76100, Israel

[b] Departamento de Fisica, Universidade Federal de Sao Carlos, Caixa Postal 676, Sao Carlos, 13565-905, SP, Brazil

Abstract

We show that non-maximally entangled states can be used to build a quantum key distribution (QKD) scheme where the key is probabilistically teleported from Alice to Bob. This probabilistic aspect of the protocol ensures the security of the key without the need of non-orthogonal states to encode it, in contrast to other QKD schemes. Also, the security and key transmission rate of the present protocol is nearly equivalent to those of standard QKD schemes and these aspects can be controlled by properly harnessing the new free parameter in the present proposal, namely, the degree of partial entanglement. Furthermore, we discuss how to build a controlled QKD scheme, also based on partially entangled states, where a third party can decide whether or not Alice and Bob are allowed to share a key.

Key words: Quantum communication, Quantum cryptography and communication security, Entanglement production and manipulation
PACS: 03.67.Hk, 03.67.Dd, 03.67.Bg

1. Introduction

The ability to communicate secretly is considered one of the most important challenges of the information era [1]. For all practical purposes most modern public key systems can be considered secure [2]. However, this security is not based on any mathematical proof but on the belief that there is no classical algorithm to factorize huge prime numbers in a reasonable amount of time. Some classical cyphers, such as the one-time pad [1], do not have

[1] rigolin@ufscar.br

the aforementioned problem. They are private key protocols whose security is entirely based on a random string of bits, the key, which only the sender (Alice) and the receiver (Bob) should know. Once the key is secretly transmitted the communication is absolutely secure. The drawback with these cyphers is that any key transmitted through a classical channel can be passively monitored. Although it may be technologically difficult to get the key without being noticed, it is in principle possible.

The solution of the key transmission problem based on the laws of physics was presented for the first time by Bennett and Brassard in a seminal work [3]. Making use of quantum channels (polarized photons) the authors theoretically showed the possibility to share a secret key with absolute security if the laws of quantum mechanics are correct. They have shown that any interference of an eavesdropper (Eve) on the quantum channel can be detected by Alice and Bob at the end of the protocol. Other interesting schemes were later proposed [4, 5], in particular the E91 protocol which was the first QKD scheme that employed maximally entangled states [4]. For an extensive review on other protocols and on experimental feasibilities we refer the reader to Ref. [6].

In this contribution we present a new QKD scheme that uses directly non-maximally entangled states (no entanglement concentration needed) and the probabilistic quantum teleportation protocol (PQT) [7, 8]. Nevertheless, the present scheme resembles the BB84 [3] rather than the E91 [4] protocol, i.e., although we make use of entanglement there is no need to check for violation of any Bell inequality to assure the security of the shared key. It is the probabilistic aspect of the PQT that guarantees the security of the teleported key and, as we show later, also allows it to be encoded in a set of orthogonal states. Note that in BB84-like protocols it is mandatory to encode the key in non-orthogonal states to make sure its transmission is secure.

In contrast to other protocols, where departure from maximal entanglement makes them inoperable, our scheme exploits partial entanglement and, using a special generalized Bell measurement, ensures flawless key distribution. Furthermore, this new QKD scheme takes advantage of a new free parameter, namely the degree of partial entanglement, that enables more control over the security and transmission rate of the protocol. Indeed, as explained later, this freedom allows us to introduce a minor modification in the QKD scheme that turns it into a controlled QKD protocol, where a third party (Charlie) has the final word on whether or not Alice and Bob are allowed to share a secret key, even after all steps of the protocol were

implemented. It is also worth mentioning that Charlie decides whether or not Alice and Bob will share a key without ever knowing it, a feature that has practical applications. We also show other possible interesting extensions of the basic protocol and how we can improve its security and the reliability of the transmitted key.

2. The tools

One important ingredient in this QKD protocol, and the one that allows it to depart from E91-like protocols, is the use of *partially* entangled states to transmit the secret key from one party to the other. Indeed, as we will show, by playing with different kinds of partially entangled states and with different joint measurement basis, Alice can teleport to Bob a secret key. The other ingredient is, as anticipated in the last sentence, the proper use of a probabilistic teleportation protocol, which allows us to harness the teleporting power of a non-maximally pure entangled state.

Let us start by recalling the PQT as developed in Ref. [7] and extended in Ref. [8]. As usual, Alice wants to teleport the following qubit to Bob,

$$|\phi^A\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are arbitrary complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Contrary to the original proposal [9] Alice and Bob now share a non-maximally entangled state, $|\Phi_n^+\rangle = N(|00\rangle + n|11\rangle)$, with $0 < |n| < 1$ and $N = 1/\sqrt{1+|n|^2}$, which naturally leads to the following orthonormal basis,

$$\begin{aligned}
|\Phi_m^+\rangle &= (|00\rangle + m|11\rangle)/\sqrt{1+|m|^2}, &(2)\\
|\Phi_m^-\rangle &= (m^*|00\rangle - |11\rangle)/\sqrt{1+|m|^2}, &(3)\\
|\Psi_m^+\rangle &= (|01\rangle + m|10\rangle)/\sqrt{1+|m|^2}, &(4)\\
|\Psi_m^-\rangle &= (m^*|01\rangle - |10\rangle)/\sqrt{1+|m|^2}, &(5)
\end{aligned}$$

with m^* denoting the complex conjugate of m and $M = 1/\sqrt{1+|m|^2}$. Using the generalized Bell states (GBS) above we can rewrite the three qubit state belonging to Alice and Bob as, $|\Phi\rangle = |\phi^A\rangle \otimes |\Phi_n^+\rangle = MN\ (|\Phi_m^+\rangle\ (\alpha|0\rangle + nm^*\beta|1\rangle) + |\Phi_m^-\rangle\ (m\alpha|0\rangle - n\beta|1\rangle) + |\Psi_m^+\rangle\ (m^*\beta|0\rangle + n\alpha|1\rangle) + |\Psi_m^-\rangle\ (-\beta|0\rangle + nm\alpha|1\rangle))$, with the first two qubits being with Alice and the last one with Bob. Alice now proceeds by implementing a generalized Bell measurement (GBM), i.e., she projects her two qubits onto one of the four GBS. (Ref.

[10] discusses three possible ways to experimentally implement a GBM.) The probability to obtain a given GBS is,

$$P_{\Phi_m^+} = \left(|\alpha|^2 + |mn\beta|^2\right)/[(1+|m|^2)(1+|n|^2)], \quad (6)$$
$$P_{\Phi_m^-} = \left(|m\alpha|^2 + |n\beta|^2\right)/[(1+|m|^2)(1+|n|^2)], \quad (7)$$
$$P_{\Psi_m^+} = \left(|n\alpha|^2 + |m\beta|^2\right)/[(1+|m|^2)(1+|n|^2)], \quad (8)$$
$$P_{\Psi_m^-} = \left(|mn\alpha|^2 + |\beta|^2\right)/[(1+|m|^2)(1+|n|^2)]. \quad (9)$$

Alice then sends Bob the result of her measurement (two bits) via a classical channel who, whereupon, applies a unitary transformation on his qubit according to this information. These transformations are the same ones given in the original teleportation protocol [9]: If Alice gets $|\Phi_m^+\rangle$ then Bob does nothing, if she gets $|\Phi_m^-\rangle$ he applies a σ_z operation, if Alice measures $|\Psi_m^+\rangle$ then Bob applies σ_x and finally for $|\Psi_m^-\rangle$ he applies $\sigma_z\sigma_x$. Here, σ_z and σ_x are the usual Pauli matrices ($\sigma_z|0(1)\rangle = +(-)|0(1)\rangle$ and $\sigma_x|0(1)\rangle = |1(0)\rangle$). After the correct transformation Bob's qubit is given by one of the following possibilities,

$$|\Phi_m^+\rangle \longrightarrow |\phi^B\rangle = \frac{\alpha|0\rangle + nm^*\beta|1\rangle}{\sqrt{|\alpha|^2 + |mn\beta|^2}}, \quad (10)$$
$$|\Phi_m^-\rangle \longrightarrow |\phi^B\rangle = \frac{m\alpha|0\rangle + n\beta|1\rangle}{\sqrt{|m\alpha|^2 + |n\beta|^2}}, \quad (11)$$
$$|\Psi_m^+\rangle \longrightarrow |\phi^B\rangle = \frac{n\alpha|0\rangle + m^*\beta|1\rangle}{\sqrt{|n\alpha|^2 + |m\beta|^2}}, \quad (12)$$
$$|\Psi_m^-\rangle \longrightarrow |\phi^B\rangle = \frac{mn\alpha|0\rangle + \beta|1\rangle}{\sqrt{|mn\alpha|^2 + |\beta|^2}}. \quad (13)$$

From now on, and without loss of generality [8], we consider n and m to be real quantities. Therefore, looking at Eqs. (11) and (12) we realize that if $n = m$ the state with Bob is $\alpha|0\rangle + \beta|1\rangle$ and the protocol works perfectly. There exist other possibilities, which come from Eqs. (10) and (13), namely, $nm = 1$ or $nm^* = 1$. But this is only possible if we have maximally entangled states since those relations imply $|n| = |m| = 1$. For $n = m$ the probability of success is simply

$$P_{suc} = P_{\Phi_n^-} + P_{\Psi_n^+} = \frac{2n^2}{(1+n^2)^2}. \quad (14)$$

Therefore, if Alice knows the entanglement of the channel, which increases monotonically with n, she can match her measurement basis ($m = n$) in order to make the protocol work with probability P_{suc}. It is important to note that if $n \neq m$ Bob obtains a different state and the protocol fails. It is this property that we explore in order to build our QKD scheme.

3. The QKD scheme

Let us assume that Bob prepares with equal probability two partially entangled states, $|\Phi^+_{n_1}\rangle = N_1(|00\rangle + n_1|11\rangle)$ and $|\Phi^+_{n_2}\rangle = N_2(|00\rangle + n_2|11\rangle)$, where $n_1 \neq n_2$ and $N_j = 1/\sqrt{1+n_j^2}$, $j = 1, 2$. For each state he keeps one qubit and send the other one to Alice (See Fig. 1). Both parties previously

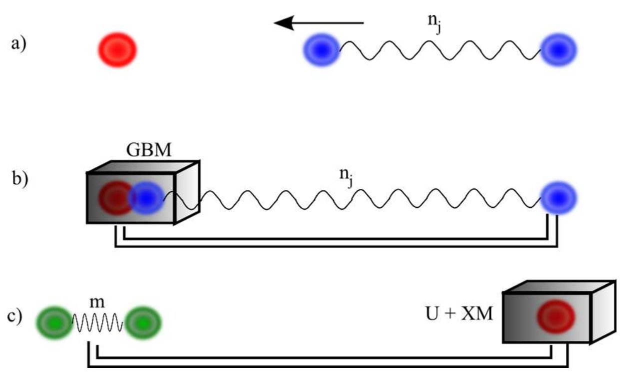

Figure 1: (Color online) Schematic representation of one run of the QKD protocol. a) Bob prepares randomly a partially entangled state, either $|\Phi^+_{n_1}\rangle$ or $|\Phi^+_{n_2}\rangle$, without telling Alice which one. Then he sends her one of the entangled qubits. b) Alice implements the PQT choosing randomly between two generalized Bell measurements (GBM). She teleports randomly either the state $|+\rangle$ or $|-\rangle$. She then tells Bob her measurement result, $|\Phi^\pm_m\rangle$ or $|\Psi^\pm_m\rangle$, but does not tell him which basis she used (if $m = n_1$ or $m = n_2$). c) With this information Bob applies the right unitary operation (U) on his qubit and projects it onto the X-basis $|\pm\rangle$ (XM). Then both parties broadcast the values of n and m. If $n \neq m$ they discard this run. If $n = m$ and Alice's GBM yielded $|\Phi^-\rangle$ or $|\Psi^+\rangle$ they both agree on the teleported qubit, which constitute one bit of the secret key.

agreed on the values of n_1 and n_2 but at this stage Bob does not tell Alice the respective value of n for each entangled state he prepared. Alice, on the other hand, prepares randomly two types of single qubit states, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, which are to be associated with the secret key she wants to share with Bob. For example, the parties use the convention that $|+\rangle$

represents the bit 0 and that $|-\rangle$ the bit 1. Note that we do not need another encoding for the bits 0 and 1 that is non-orthogonal to the previous one, as required by the BB84 protocol [2]. Alice then uses each qubit received from Bob to implement the PQT for each one of her randomly generated states $|\pm\rangle$. In doing so, she also chooses in a random way whether to project each pair of qubits (hers and Bob's) to the GBS with $m = n_1$ or $m = n_2$. Alice, however, does not inform Bob of the value of m but only which GBS she gets. At the end of this stage Bob knows what her measurement results were (but not m), which allows him to implement the right unitary operation on his qubits. After that, each one of his qubits are described by one of the four states given by Eqs. (10)-(13), with $\alpha = \beta = 1/2$.

The last six steps of the protocol are as follows. First, Bob projects his qubits onto the $|\pm\rangle$ basis. Second, Bob and Alice reveal in a public channel the following information. Bob tells Alice which value of n (n_1 or n_2) he has assigned to each partially entangled state whilst Alice tells him the value of m (n_1 or n_2) for each GBM she made. Third, they keep all the cases where she has rightly matched the entanglement of the channel with the entanglement of the measuring basis, i.e., whenever the shared entangled state was $|\Phi^+_{n_j}\rangle$ and Alice chose $m = n_j$, $j = 1, 2$. Fourth, they discard all the other cases since the PQT fails there ($m \neq n_j$). Fifth, within the cases where the matching condition is satisfied, Bob and Alice keep only those instances where her measurement results were $|\Phi^-\rangle$ or $|\Psi^+\rangle$, the so called successful runs of the PQT. For those, and only those runs of the protocol, Alice and Bob are sure they agree on the teleported state and consequently on the random string of zeros and ones. Finally, the last step consists of using half of the successful cases to test whether or not Eve has tried to tamper with the key.

In an idealized situation, i.e., perfect detectors and no noise, they simply broadcast half of their valid results in a public classical channel and check if they always get the same bits. If they do, the remaining half of bits are their secret key. If they fail to agree on the public data, they discard everything and repeat the whole protocol again. However, noise and non-ideal detectors will introduce some errors even when all the steps of the protocol are successful.

[2] We could have chosen another encoding for the bits 0 and 1. This would increase the security of the present protocol on the expense of the key transmission rate. However, as it is clear from the security analysis, this is not mandatory.

Nevertheless, Alice and Bob can still achieve any desired level of security by increasing the size of the shared key and employing classical reconciliation protocols and privacy amplification techniques already developed for other QKD schemes [11].

Assuming an ideal scenario, for instance, excellent detectors and efficient measurement processes, we can calculate the maximum rate of how many teleported qubits constitute the final secret key. We know that Alice implements the PQT half of the times making a GBM with $m = n_1$ and half with $m = n_2$. Therefore, the total probability of success for all PQT is, according to Eq. (14), $n_1^2/(1+n_1^2)^2 + n_2^2/(1+n_2^2)^2$. But half of the successful cases are discarded to check for the presence of Eve, and the final rate becomes

$$P_{suc}^{final} = \frac{n_1^2}{2(1+n_1^2)^2} + \frac{n_2^2}{2(1+n_2^2)^2}. \tag{15}$$

On the other hand, if we look at the BB84 protocol [3], we see that half of the times Bob measures the qubits he receives from Alice using the same basis she employed to prepare them and, within these successful runs, the other half is used to test for the security of the protocol. This gives us, assuming no loss during the transmission of the qubit and ideal detectors, a total idealized rate of 1/4. Returning to the protocol presented here, it is not difficult to see that $P_{suc}^{final} < 1/4$, no matter what the values of n_1 and n_2 are. (If they are equal to one we have 1/4 but then the protocol is useless.) However, for modest values of n_1 and n_2 (a little greater than 0.5) we get rates above 15%. If we allow one of them to approach unity we do even better. For example, if we have $n_1 = 0.5$ and $n_2 = 0.9$ we already obtain rates higher than 20%.

There exists, nevertheless, an important feature that we can easily achieve employing this protocol that is unattainable using the BB84 protocol. We can transform it into a sort of controlled QKD scheme introducing another party (Charlie) who can decide whether or not Alice and Bob are allowed to share a secret key even after they finished all steps of the protocol. In order to do that, we let Charlie prepare and distribute the entangled states $|\Phi_{n_1}^+\rangle$ and $|\Phi_{n_2}^+\rangle$ to Alice and Bob. Hence, if Charlie publicly announces the values of n for each entangled state he prepared he can make the protocol work without ever knowing the key. Otherwise, if he does not broadcast this information, the protocol ultimately fails. Note that the probability of success in this scenario, assuming Charlie broadcast all the values of n for each entangled pair he prepares, is the same we had before, Eq. (15). His role here is simply to distribute the entangled states between Alice and Bob,

without changing the final success rate for the protocol. We also remark that a similar third party control can be achieved using a different QKD scheme based on maximally entangled Bell states [12].

At this point we wish to emphasize the main differences between the present scheme and the BB84 and the E91 protocol. As described above, here we can achieve a level of third party control that is unattainable using the former two protocols. This is an important and practical characteristic of this scheme that, as we show below, can also be extended to a fourth, fifth, $\ldots$, n-th party level of control. Moreover, in the present protocol the key is never transmitted from Alice to Bob as in the BB84 protocol. Rather, it is teleported from one party to the other, which gives an additional flexibility for this protocol in its third party formulation. Indeed, once Alice and Bob have shared the partially entangled states distributed by Charlie they can easily exchange their roles. Instead of Alice teleporting the key to Bob, he is the one who teleports the key to her. Also, contrary to the E91 protocol where a maximally entangled state is directly responsible to the generation of the secret key, here we use a non-maximally entangled state as a channel through which the key is teleported. In other words, the non-maximally entangled states of the present scheme have no direct role on the generation of the secret key.

4. Security

The security of this protocol is based on the same premises of the BB84 protocol and, therefore, we can understand the security of the former by recalling the security analysis [3] of the latter. The key ingredient here is the recognition that there are two unknown sets of actions throughout the implementation of the BB84 protocol that are only publicly revealed at the end of it: the basis in which Alice prepared her qubits and the basis in which Bob measured the qubits received from Alice. A similar thing happens for the present protocol. We have two unknown sets of actions throughout each run of the protocol that are revealed only at its end: the entanglement of the shared qubits between Alice and Bob and what basis Alice used to implement the GBM. This lack of information prevents Eve from always obtaining the right bit being sent from Alice to Bob without being noticed. As we show below, the laws of quantum mechanics forbid Eve from acquiring information about the key being transmitted without disturbing the quantum

state carrying it if she does not know which entangled state is shared between Alice and Bob.

Let us assume, for definiteness, that in one of the runs of the protocol Alice prepared the state $|+\rangle$ and that Eve, somehow, replaced the entangled state produced by Bob with one produced by her. Eve wants the state prepared by Alice to be teleported to her. By doing so she thinks she can obtain information on the key. However, she does not know which GBM Alice implemented to perform the PQT ($m = n_1$ or $m = n_2$). This information is only revealed after Bob confirms he measured his qubit. She only knows that the measurement result of Alice is, say, $|\Phi^-\rangle$. (This is the best scenario for Eve.) Therefore, Eve's qubit is described by Eq. (11), $|\phi^E\rangle = \frac{m|0\rangle+n|1\rangle}{\sqrt{m^2+n^2}}$, which can be written as,

$$|\phi^E\rangle = \frac{1}{\sqrt{2(m^2+n^2)}}\left[(m+n)|+\rangle + (m-n)|-\rangle\right]. \tag{16}$$

Looking at Eq. (16) we see that unless Eve guessed correctly Alice's choice for m (and this only happens half of the times), preparing the right entangled state with $n = m$, we have a superposition of the states $|+\rangle$ and $|-\rangle$. This implies that she obtains the wrong bit being transmitted with probability $P_{wrong} = (m-n)^2/(2(m^2+n^2)) = 1/2 - mn/(m^2+n^2)$. In other words, since we have a superposition of the right and wrong answers quantum mechanics forbids Eve from always getting the right one with a single measurement. It is clear now that this is similar to the argument used to prove the security of the BB84 protocol. Hence, no matter what Eve does, if she prepared the wrong entangled state and Bob the right one, she will be caught trying to tamper with the key when Alice and Bob publicly compare part of it. This is true since Eve cannot with certainty send Bob another qubit which mimics the right one. Furthermore, Eq. (16) tells us that the greater the difference between n_1 and n_2 the more likely will Eve be detected. We can see this by noting that P_{wrong} increases as a function of $|m-n|$ or, equivalently, as a function of the difference in entanglement between the channels. Lastly, the chances of Eve being caught also increases with the size of the string of bits being publicly announced.

We can also estimate the optimal range of parameters (n_1 and n_2) for this protocol, assuming we want to maximize the transmission rate while at the same time minimizing the chances of Eve guessing the correct qubit being teleported. In other words, we want to maximize a function proportional to

$P_{wrong}P_{suc}$, where P_{wrong} is, as given above, the probability of Eve guessing the wrong qubit and P_{suc} is Eq. (15), the total rate of success in the transmission of the key. Both P_{wrong} and P_{suc} are now considered functions of n_1 and n_2. A simple numerical analysis shows that the best strategies occur for $n_1 \approx 1$ and $n_2 \approx 0$ (and vice-versa), while the worst cases for Alice and Bob occur when $n_1 \approx n_2$.

Note that the security check outlined above is an idealization. In real-life situations we always have noise and imperfect devices that give wrong answers even in the absence of Eve. However, this can be controlled using classical reconciliation protocols and privacy amplification [11]. A more detailed security analysis based on bounds for the mutual information between Alice, Bob, and Eve using, for example, the techniques of Refs. [13, 14], is beyond our goals here and is left for future work.

5. Extensions of the QKD scheme

The QKD scheme presented here is very versatile and allows for arbitrary control over the protocol parameters. This can be achieved by introducing two extensions, where one increases its security and the other increases the distance of reliable transmission of the key. The security of the protocol is increased by allowing Bob to generate more than two partially entangled states. For example, instead of just creating the states $|\Phi^+_{n_j}\rangle$, $j = 1, 2$, he can create three or more states with different n. With only two states, Eve can guess the right GBM in half of the successful runs of the PQT. However, with more entangled states, her chances are reduced to $1/N$, where N is the number of partially entangled states produced by Bob. On the other hand, this increase in security reduces the transmission rate of the key since it becomes less likely that Alice and Bob achieve the matching condition $(m = n)$.

To extend the distance of reliable key transmissions we can use quantum repeater [15] stations. In this scenario it is the first station (the closest to Alice) that generates the partially entangled states and then publicize the values of n, only after Bob measures his qubits. The other stations use maximally entangled states to successively teleport Alice's qubit to Bob. Note that security increases if other repeater stations use partially entangled states too. The repeater stations can also be used to extend the third party control described before to any number of parties. Indeed, if we allow each station to freely choose its own partially entangled states we are increasing

the number of parties that can decide whether or not Alice and Bob will share a secret key. This is true for the protocol will work if, and only if, all the repeater stations disclose to Alice and Bob which partially entangled states they generated at each run of the protocol.

6. Experimental feasibility

While noise and decoherence of entangled qubits usually result in mixed states [16, 17], partially-entangled states used in the aforementioned QKD protocol can be considered in the scenario of coupling to a zero-temperature bath [18]. In this regime dynamical control of decoherence [19, 20, 18] allows one to determine the amount of partial entanglement of the channel by properly tuning the relative decoherence between the qubits. Thus, the party sending the partially entangled states (either Bob in the standard QKD or Charlie in the controlled version) can select the degree of partial entanglement and is not restricted by the amount of noise in the system.

7. Summary

We showed that partially entangled states are useful resources for the construction of a direct QKD scheme by the proper use of probabilistic teleportation protocols. This has an interesting implication on the practical implementation of entangled based QKD schemes, as it is extremely difficult to produce maximally entangled qubits. Using the protocol presented here, one can alleviate the experimental demands on the production of entangled pairs without rendering QKD inoperable. Furthermore, the present partially entangled state based QKD scheme is flexible enough that we were able extend it in at least three directions, each one augmenting its usability. The first one turned the protocol into a controlled QKD scheme, where a third party decides whether or not Alice and Bob are able to share a secret key. Then we demonstrated how one can increase its security by letting the parties use more and more different partially entangled states to implement one of the steps of the QKD protocol, namely, the probabilistic teleportation protocol. And third, we discussed how the use of quantum repeaters extends the distance of reliable key transmission without diminishing the key rate.

Finally, the present QKD protocol naturally leads to new interesting questions. For instance, can we increase the key transmission rate using partially entangled qudits instead of qubits? Is there any possible way of devising a

similar approach using mixed entangled states? Or using continuous variable entangled systems? Can we do better by using different types of entangled qubit-like states, such as the cluster state [21] or the cluster-type coherent entangled states [22]? It is our hope that the ideas presented here might lead to clues on how to answer these questions.

Acknowledgments

G. R. thanks the Brazilian agency Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) for funding this research.

References

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (First Anchor Books Edition, New York, 2000)

[2] R. Rivest, A. Shamir, and L. Adleman, *MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, 1979*

[3] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing* (Proceedings of IEEE International Conference on Computers Systems and Signal Processing: Bangalore, India, 1984) p. 175

[4] A. K. Ekert, *Phys. Rev. Lett.* **67** (1991) 661

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **68** (1992) 557

[6] W. Tittel, H. Zbinden, and N. Gisin, *Phys. Rev. A* **63** (2001) 042301

[7] P. Agrawal and A. K. Pati, *Phys. Lett. A* **305** (2002) 12

[8] G. Gordon and G. Rigolin, *Phys. Rev. A* **73** (2006) 042309

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70** (1993) 1985

[10] H. Kim, Y. Cheong, and H. Lee, *Phys. Rev. A* **70** (2004) 012309

[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5** (1992) 3

[12] T. Durt, A. L.-Linares, A. Ling, and C. Kurtsiefer, *Phys. Rev. A* **78** (2008) 042338.

[13] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, *Phys. Rev. A* **62** (2000) 012302

[14] E. Karpov, P. Navez, and N. J. Cerf, *Phys. Rev. A* **72** (2005) 042314

[15] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81** (1998) 5932

[16] T. Yu and J. H. Eberly, *Phys. Rev. Lett.* **93** (2004) 140404

[17] G. Gordon, *Eur. Phys. Lett.* **83** (2008) 30009

[18] G. Gordon and G. Kurizki, *Phys. Rev. Lett.* **97** (2006) 110503

[19] A. G. Kofman and G. Kurizki, *Nature (London)* **405** (2000) 546

[20] G. Gordon, G. Kurizki, and D. A. Lidar, *Phys. Rev. Lett.* **101** (2008) 010403

[21] H. J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86** (2001) 910

[22] P. P. Munhoz, F. L. Semião , A. Vidiella-Barranco, and J. A. Roversi, *Phys. Lett. A* **372** (2008) 3580